Benefits from Implementing the Framework:

- Enables agencies to develop a benchmark to gauge year-to-year progress across the Framework’s functions and categories.
- Provides organizations with metrics to see how they rate compared to similar organizations.
- Informs C-level/executive management about an agency’s security program/resource needs using the NIST Cybersecurity Framework (CSF) language.
- Assists with education and awareness for security staff.
- Aids in establishing priorities for security program tasks.
- Allows an organization to manage cybersecurity risk more systematically.
- Helps to standardize security requirements for collaboration (i.e., data exchange) among feds, states and local/tribal peers.

Drivers

- In 2013, DHS partnered with the MS-ISAC to annually conduct the NCSR. The MS-ISAC was selected because it collaborates with SLTT governments on cybersecurity risk and incidents.
- In 2014, after the NIST Cybersecurity Framework was released, the 2015 NCSR was updated to align with the CSF in an effort to increase standardization and use of a common language across the SLTT community.
- The CSF was selected as it provides a concise, easy-to-use language that was already validated and supported by a community of cybersecurity experts.

Situation

- The Multi-State Information Sharing and Analysis Center (MS-ISAC) helps State, Local, Territorial, and Tribal (SLTT) entities share best practices and provides guidance to help them improve their cybersecurity program.
- In June 2009, the U.S. Department of Homeland Security (DHS) was directed by Congress to develop a cyber-network security assessment that would measure gaps and capabilities of state, local, tribal and territorial governments’ cybersecurity programs. In 2011, this first version of the self-assessment became known as the Nationwide Cybersecurity Review (NCSR). The self-assessment allows state, local, tribal and territorial governments (SLTT) governments to manage cybersecurity related risk through the NIST CSF, which consists of best practices, standards, and guidelines.
- Through the NCSR, DHS and MS-ISAC examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk.
- Every other year, the NCSRS Summary Report, which is based on the CSF, is sent to Congress.
- The CSF filled the need for a standardized language for reporting cybersecurity maturity to share implementation metrics across the SLTT community.

---

There are many available standards our cybersecurity community may utilize to guide an agency in their quest for furthering its cybersecurity program. With NIST’s Cybersecurity Framework (CSF) designated as a tool federal agencies should use, our local community, across the Nation, was incentivized to also follow the Framework. The NIST CSF has served as a superb standard to enable all agencies to be on the same ‘measurement’ page. This allows agencies to be measured and evaluated equally. The adoption of the NIST CSF for MS-ISAC’s Nationwide Cybersecurity Review (NCSR) was a huge step in improving our state, local, tribal and territorial (SLTT) communities’ metric of year-to-year and peer-to-peer comparisons on a national scale.

As CISO to both Napa and Mono Counties (California), I have greatly benefited by using NIST’s CSF in conjunction with MS-ISAC’s NCSR. The majority of California counties have also adopted NIST’s CSF as the appropriate tool for our statewide standard.”

- Gary Coverdale, CISO
Process
Organizations have a desire and need to understand, strengthen and/or sustain their level of cybersecurity maturity.

- The NCSR assessment is available on an annual basis, from October 1, through December 15.
- Users complete the NCSR self-assessment by assessing how their organization is addressing the different activities within CSF.
- They use the risk assessment and identified gaps to determine priorities within a security program.
- By relying on the Cybersecurity Framework core, agencies ensure they are tracking year-to-year and peer-to-peer progress.

Framework Implementation Overview
- DHS, through the MS-ISAC, leverages the Cybersecurity Framework to standardize cybersecurity concepts to measure cybermaturity of an SLTT.
- SLTTs use the Cybersecurity Framework through the NCSR self-assessment to monitor improvements year-over-year.
- MS-ISAC coordinates with SLTTs to register them for the NCSR and to assist in reviewing the results of their assessment.

Results and Impacts
- The results of the NCSR are frequently used to measure compliance within an organization’s security and privacy programs.
- By developing a cybersecurity maturity baseline against the Cybersecurity Framework core, many organizations reported that they are able to use the NCSR to measure their Cybersecurity posture/maturity.
- Participating SLTT agencies have reported that they are able to use the NCSR metrics and the common language of the Cybersecurity Framework core to effectively convey their cybersecurity status and/or need to C-level executives and/or board members.
- Federal Emergency Management Agency (FEMA) recognizes the use of the NCSR, based on the Cybersecurity Framework, as a tool for evaluating applications for cybersecurity grant funding opportunities.

What’s Next?
- Continue to educate and assist the SLTT community in understanding the gaps and capabilities within their cybersecurity programs.
- The MS-ISAC and DHS will continue to work together to assist the SLTT community in improving agencies’ overall cybersecurity posture.
- Continuously work with NIST to reflect the changes and additions to the Cybersecurity Framework within the NCSR question set.

Contact Information & Resources
Multi-State Information Sharing & Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/services/ncsr/
NCSR@cisecurity.org or 518-880-0736
Cybersecurity Framework website:
https://www.nist.gov/cyberframework
NIST contact: cyberframework@nist.gov